FIG. 1

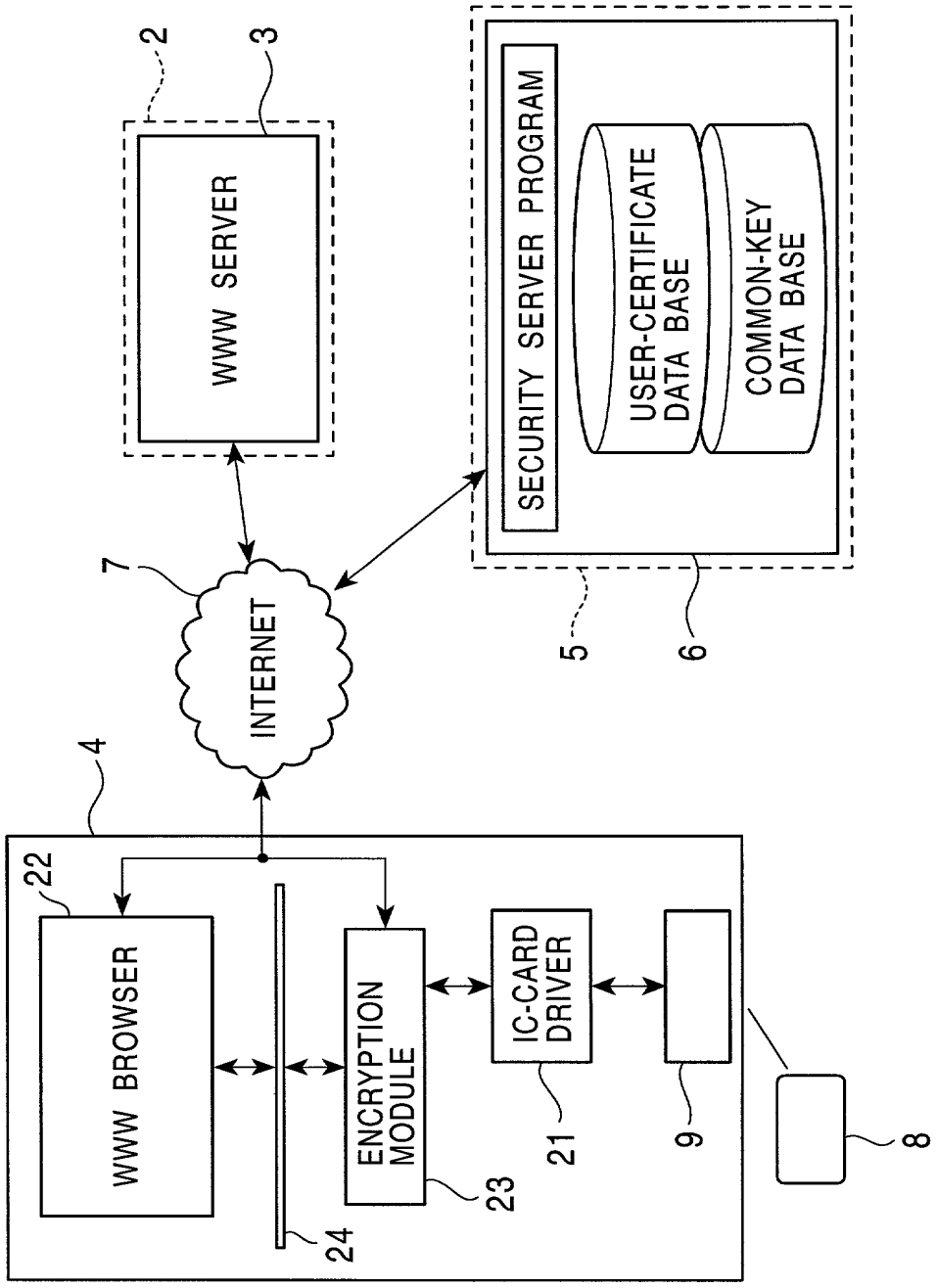

2
3
WWW SERVER
SECURITY SERVER PROGRAM
USER-CERTIFICATE DATA BASE
COMMON-KEY DATA BASE
7
INTERNET
5
6
4
22
WWW BROWSER
ENCRYPTION MODULE
IC-CARD DRIVER
21
9
8
23
24

FIG. 2

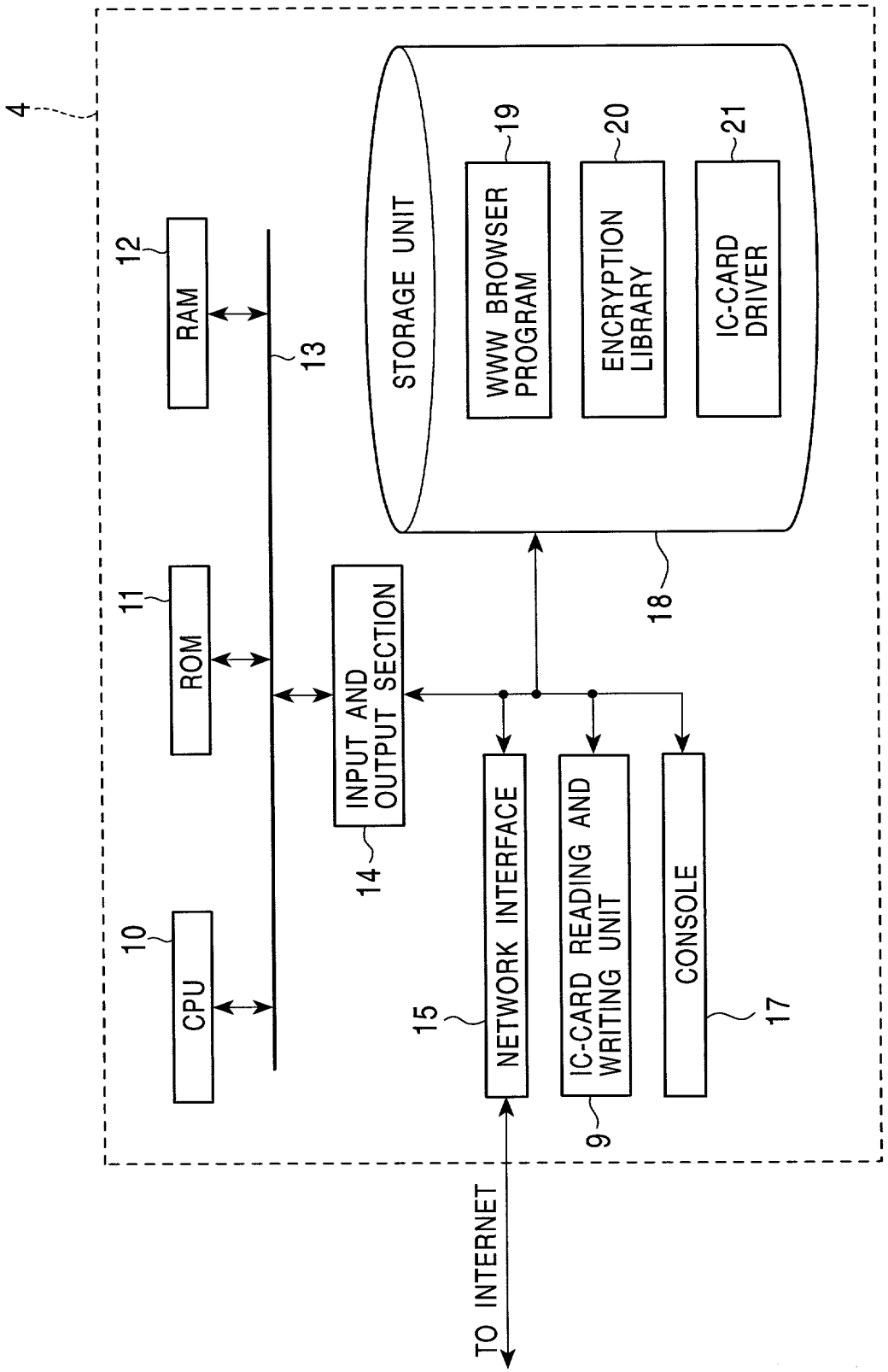

4
STORAGE UNIT
WWW BROWSER PROGRAM
19
ENCRYPTION LIBRARY
20
IC-CARD DRIVER
21
18
RAM
12
13
ROM
11
INPUT AND OUTPUT SECTION
14
CPU
10
NETWORK INTERFACE
15
IC-CARD READING AND WRITING UNIT
9
CONSOLE
17
TO INTERNET

FIG. 3

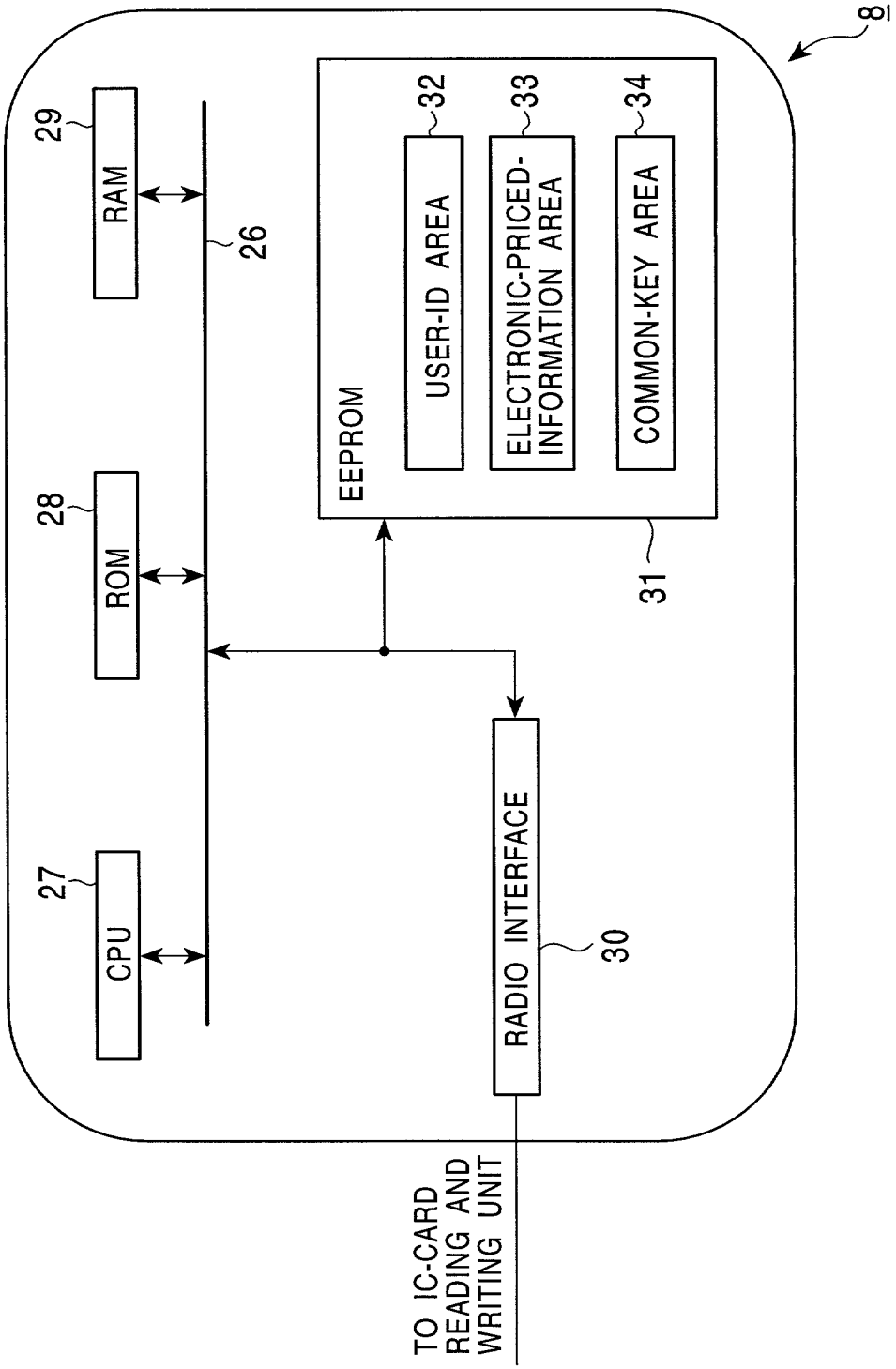

8
29
RAM
26
28
ROM
27
CPU
EEPROM
32
USER-ID AREA
33
ELECTRONIC-PRICED-INFORMATION AREA
34
COMMON-KEY AREA
31
RADIO INTERFACE
30
TO IC-CARD READING AND WRITING UNIT

FIG. 4

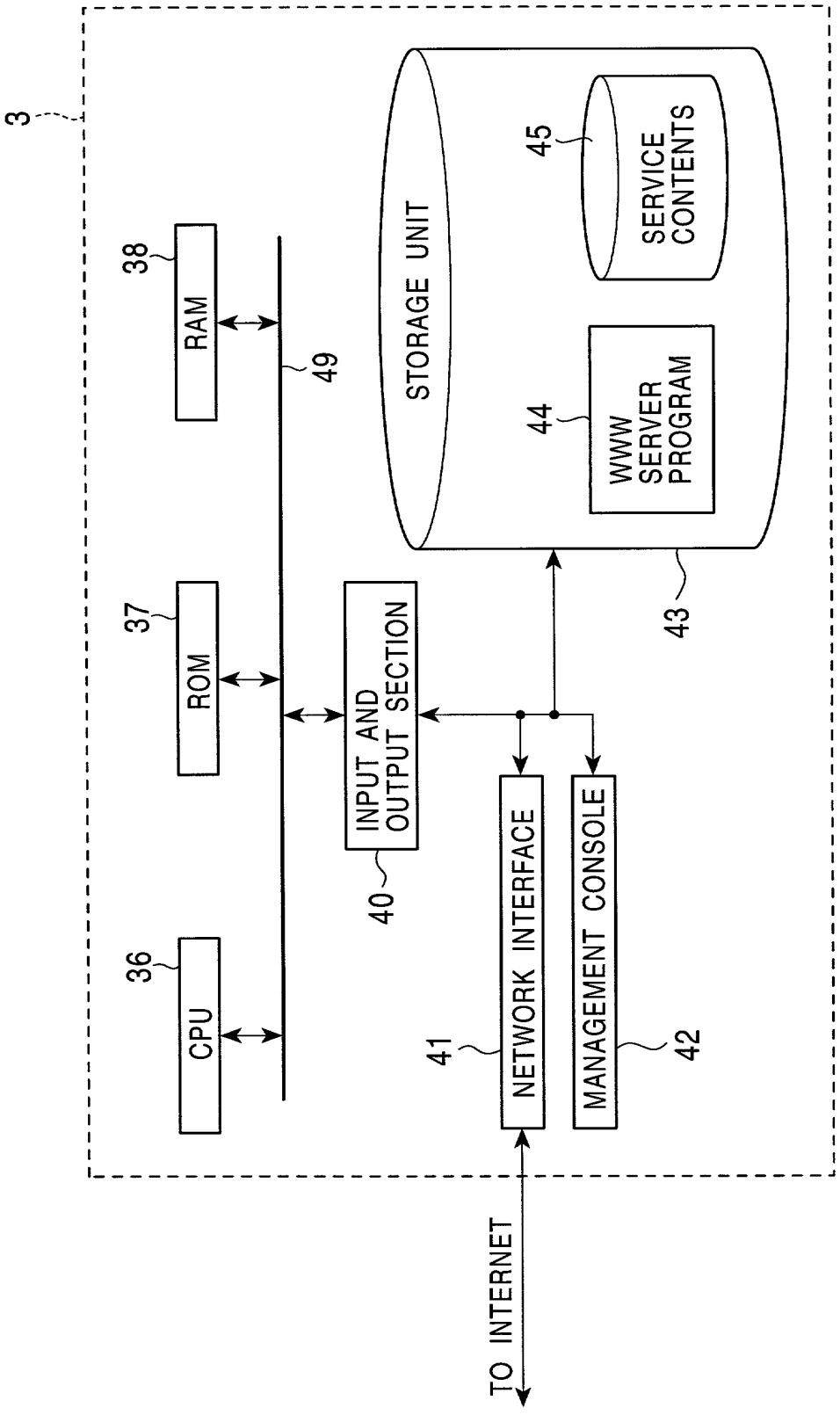

3
38
RAM
49
37
ROM
36
CPU
INPUT AND OUTPUT SECTION
40
41
NETWORK INTERFACE
MANAGEMENT CONSOLE
42
TO INTERNET
STORAGE UNIT
43
44
WWW SERVER PROGRAM
45
SERVICE CONTENTS

FIG. 5

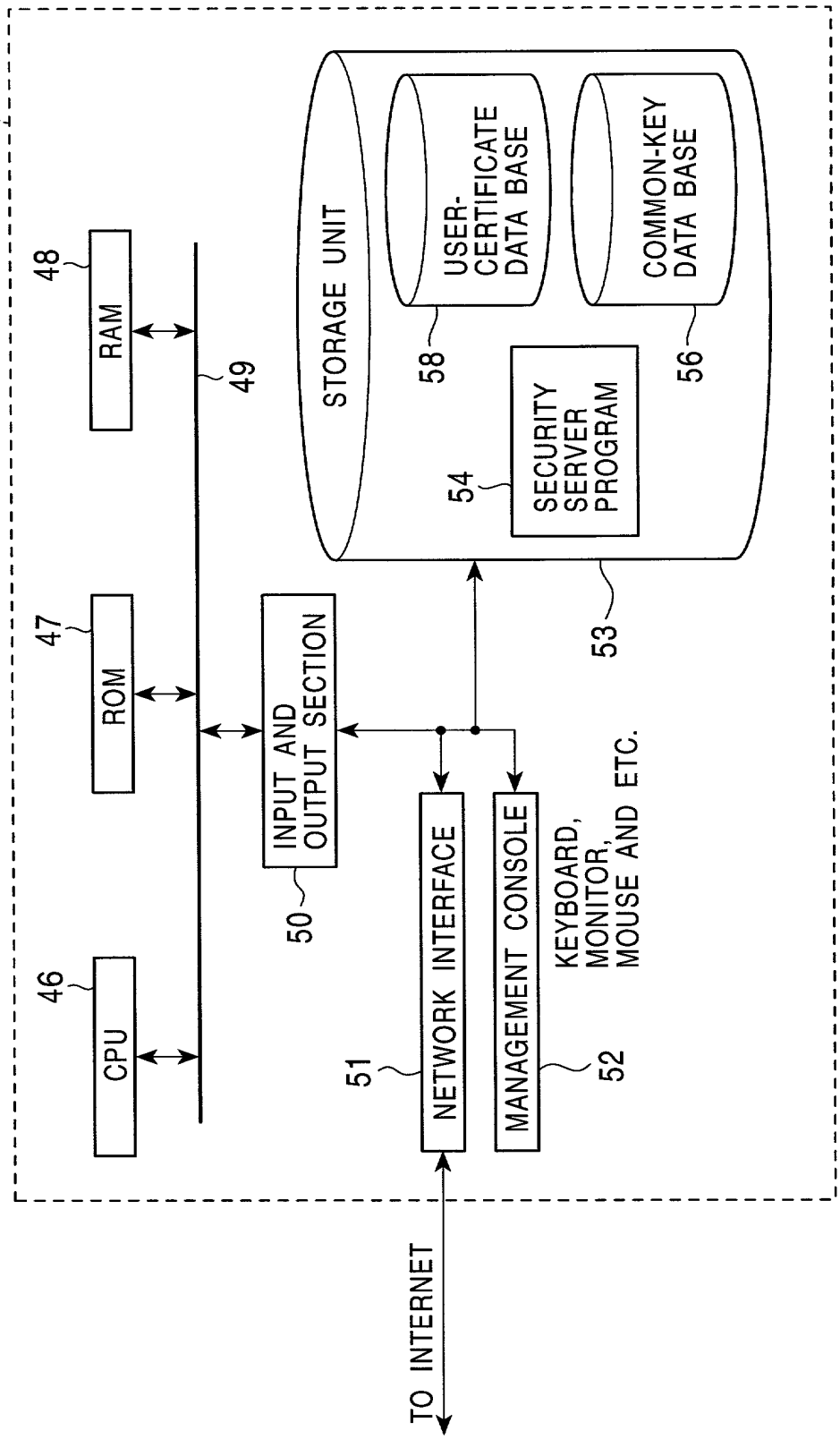

6
48
RAM
49
47
ROM
46
CPU
50
INPUT AND OUTPUT SECTION
51
NETWORK INTERFACE
52
MANAGEMENT CONSOLE
KEYBOARD, MONITOR, MOUSE AND ETC.
TO INTERNET
STORAGE UNIT
53
58
USER-CERTIFICATE DATA BASE
56
COMMON-KEY DATA BASE
54
SECURITY SERVER PROGRAM

FIG. 6

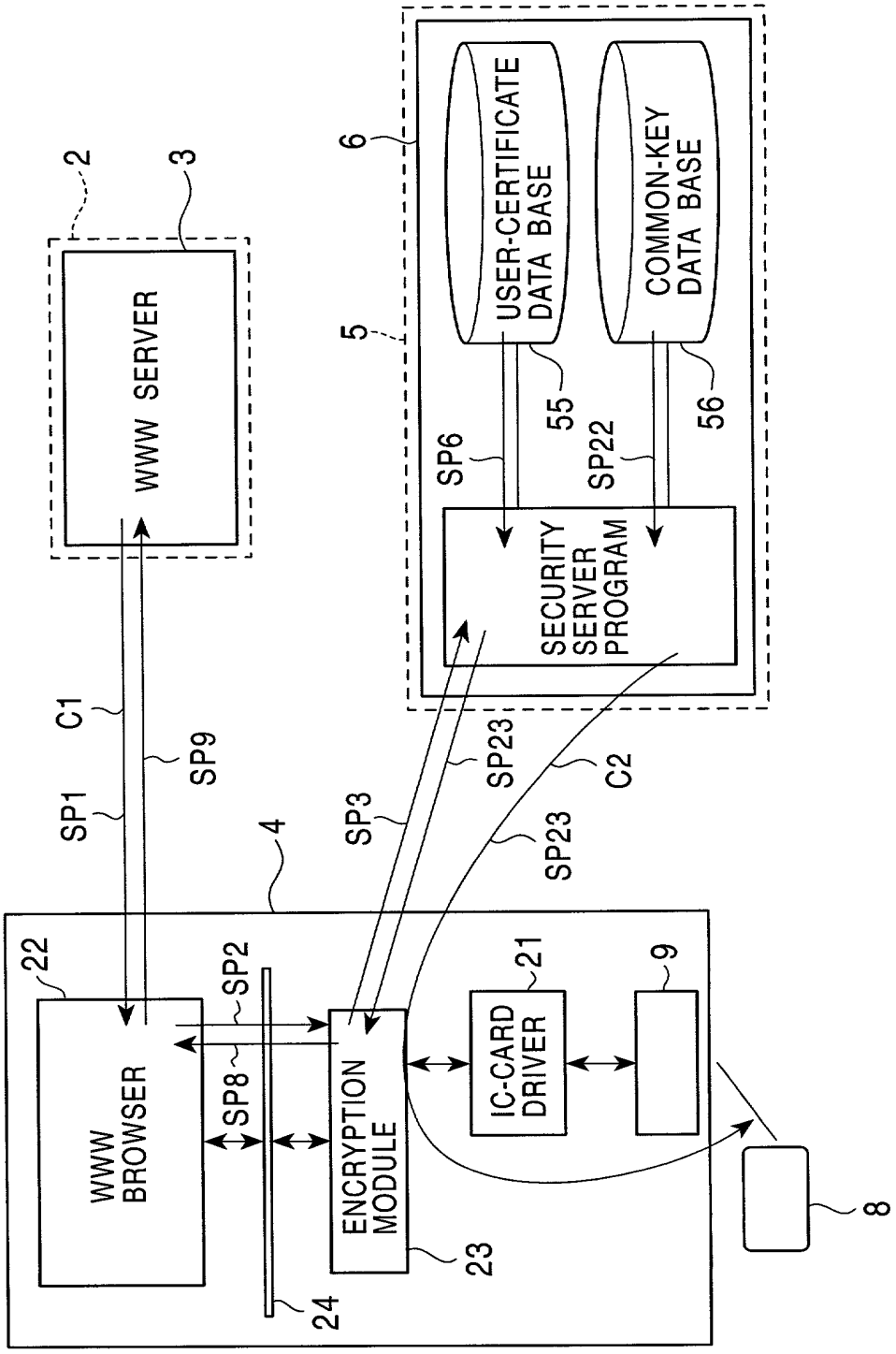

2
3
WWW SERVER
6
USER-CERTIFICATE DATA BASE
COMMON-KEY DATA BASE
5
55
56
SP6
SP22
SECURITY SERVER PROGRAM
C1
SP1
SP9
SP3
SP23
C2
SP23
4
22
SP2
SP8
WWW BROWSER
ENCRYPTION MODULE
21
IC-CARD DRIVER
9
23
24
8

FIG. 7

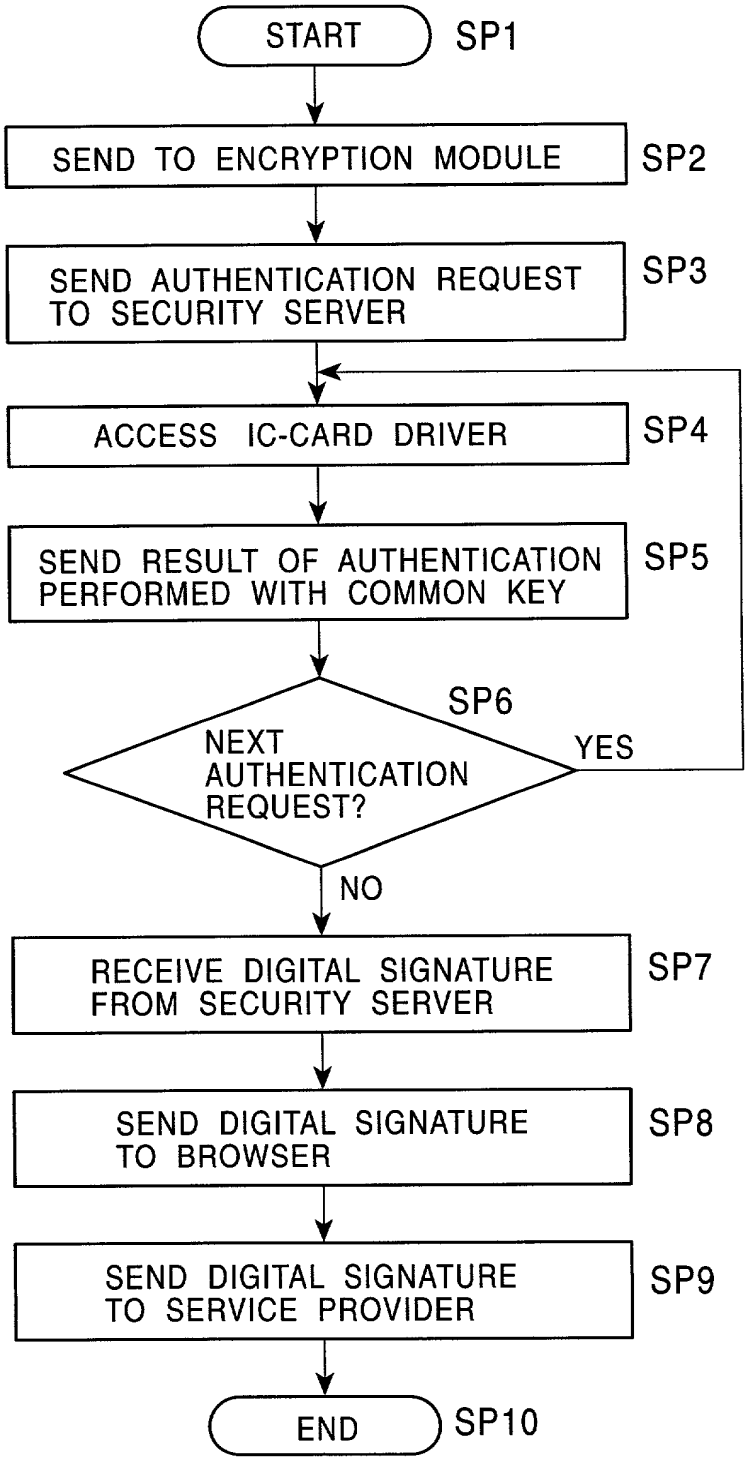

START
SP1
SEND TO ENCRYPTION MODULE
SP2
SEND AUTHENTICATION REQUEST TO SECURITY SERVER
SP3
ACCESS IC-CARD DRIVER
SP4
SEND RESULT OF AUTHENTICATION PERFORMED WITH COMMON KEY
SP5
SP6
NEXT AUTHENTICATION REQUEST?
YES
NO
RECEIVE DIGITAL SIGNATURE FROM SECURITY SERVER
SP7
SEND DIGITAL SIGNATURE TO BROWSER
SP8
SEND DIGITAL SIGNATURE TO SERVICE PROVIDER
SP9
END
SP10

FIG. 8

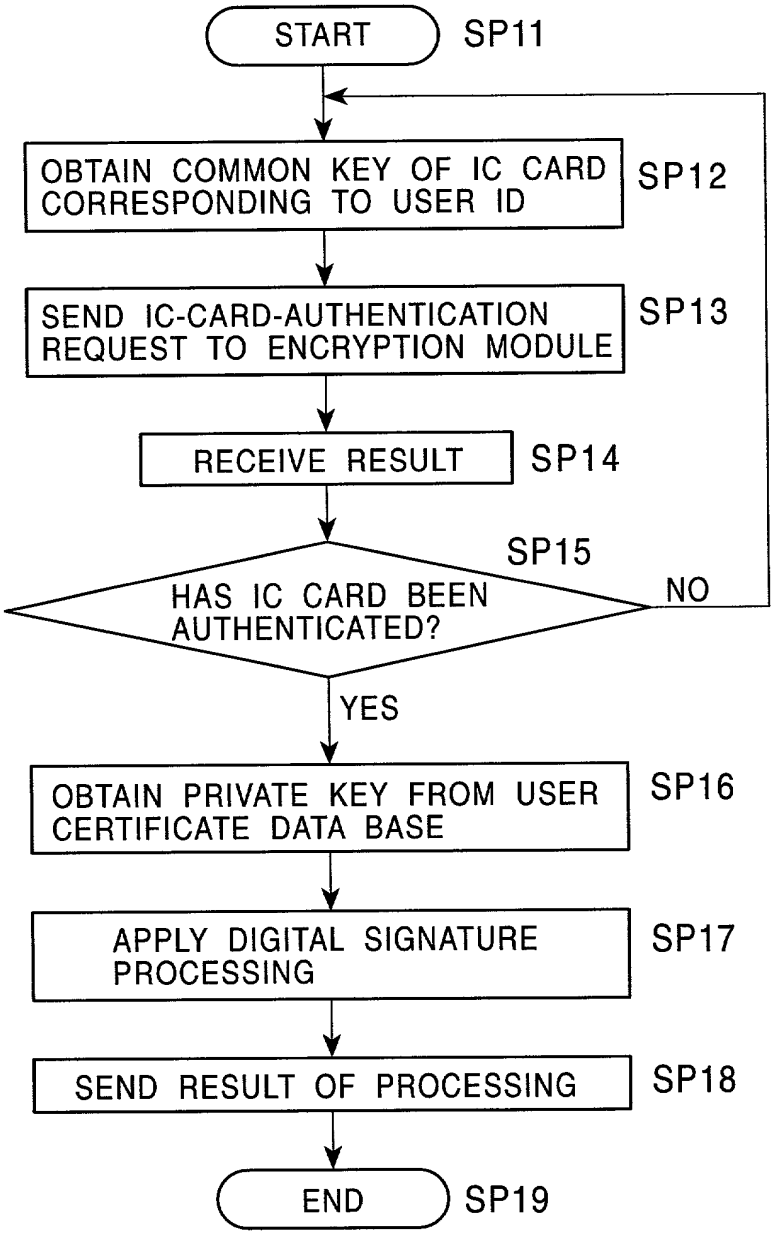

START
SP11
OBTAIN COMMON KEY OF IC CARD CORRESPONDING TO USER ID
SP12
SEND IC-CARD-AUTHENTICATION REQUEST TO ENCRYPTION MODULE
SP13
RECEIVE RESULT
SP14
SP15
HAS IC CARD BEEN AUTHENTICATED?
NO
YES
OBTAIN PRIVATE KEY FROM USER CERTIFICATE DATA BASE
SP16
APPLY DIGITAL SIGNATURE PROCESSING
SP17
SEND RESULT OF PROCESSING
SP18
END
SP19

FIG. 9

USER ID	COMMON KEY FOR IC CARD
0001	XXXXXXXXXXXX
0002	XXXXXXXXXXXX
0003	XXXXXXXXXXXX
⋮	⋮

56

FIG. 10

57 USER ID	58 CERTIFICATE	59 PRIVATE KEY
0001	CERTIFICATE CORRESPONDING TO USER ID 0001	XXXXXXXXXXXX
0002	CERTIFICATE CORRESPONDING TO USER ID 0002	XXXXXXXXXXXX
0003	CERTIFICATE CORRESPONDING TO USER ID 0003	XXXXXXXXXXXX
⋮	⋮	⋮

55

FIG. 11

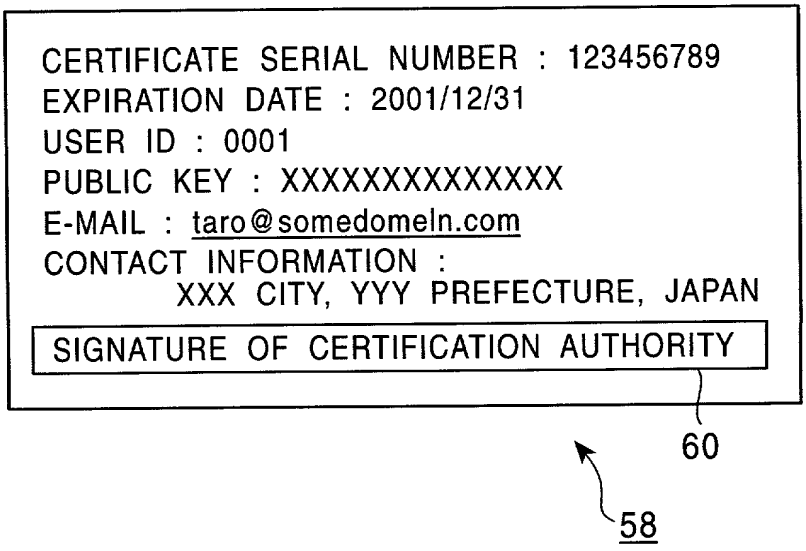

CERTIFICATE SERIAL NUMBER : 123456789
EXPIRATION DATE : 2001/12/31
USER ID : 0001
PUBLIC KEY : XXXXXXXXXXXXX
E-MAIL : taro@somedomeln.com
CONTACT INFORMATION :
XXX CITY, YYY PREFECTURE, JAPAN
SIGNATURE OF CERTIFICATION AUTHORITY
60
58

FIG. 12

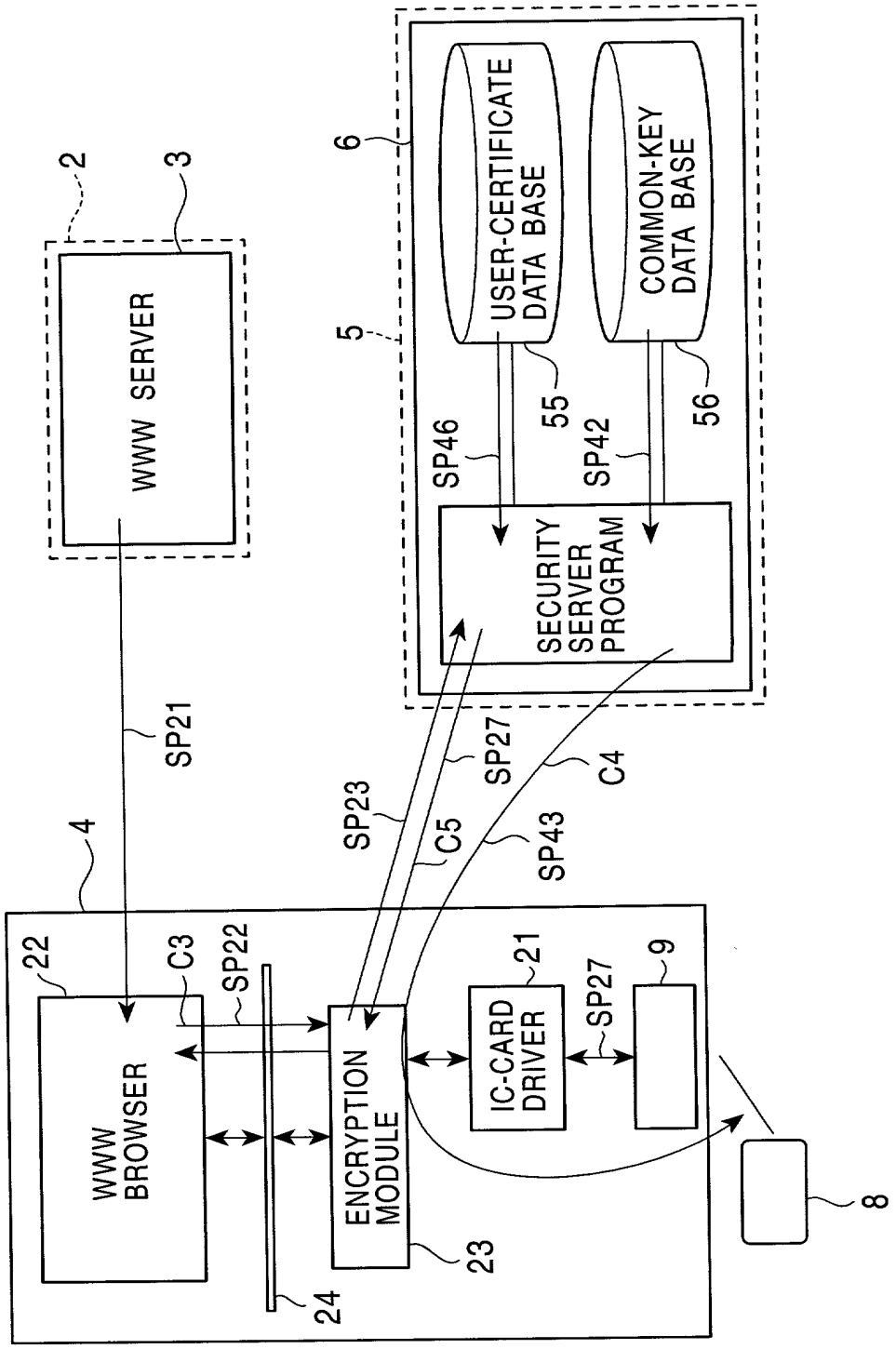

2
3
WWW SERVER
6
5
USER-CERTIFICATE DATA BASE
COMMON-KEY DATA BASE
55
56
SP46
SP42
SECURITY SERVER PROGRAM
SP21
SP23
SP27
C4
C5
SP43
4
22
C3
SP22
WWW BROWSER
ENCRYPTION MODULE
IC-CARD DRIVER
21
SP27
9
8
23
24

FIG. 13

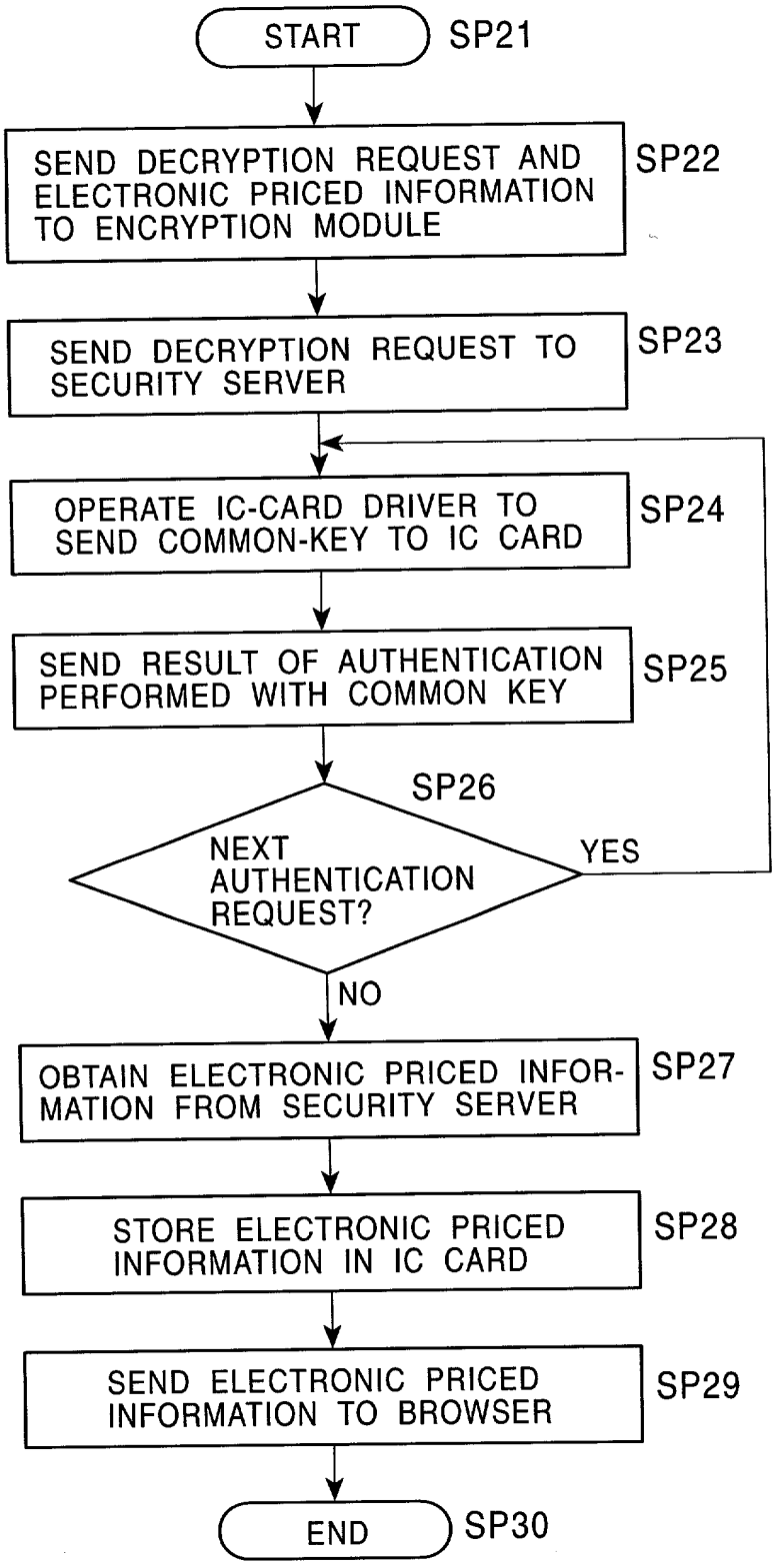
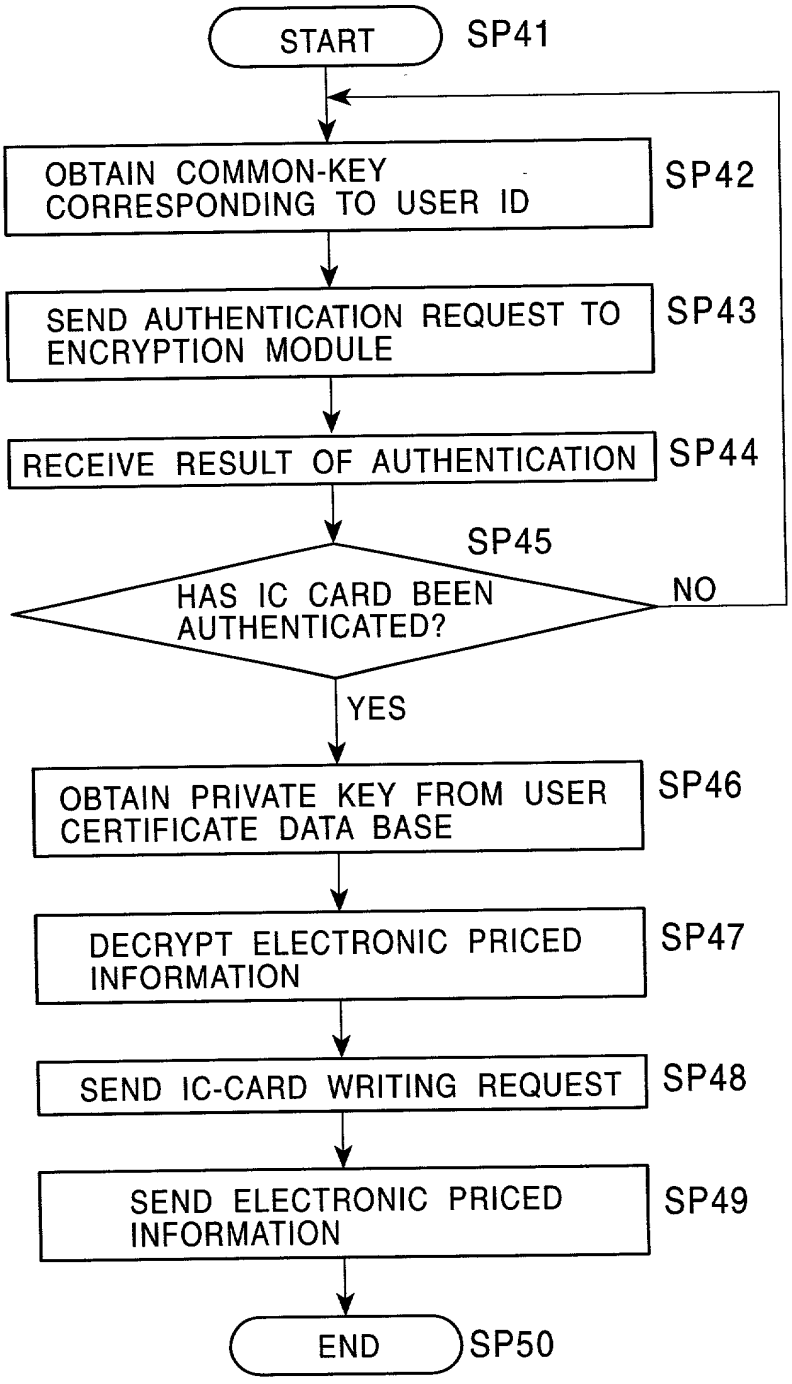

START
SP21
SEND DECRYPTION REQUEST AND ELECTRONIC PRICED INFORMATION TO ENCRYPTION MODULE
SP22
SEND DECRYPTION REQUEST TO SECURITY SERVER
SP23
OPERATE IC-CARD DRIVER TO SEND COMMON-KEY TO IC CARD
SP24
SEND RESULT OF AUTHENTICATION PERFORMED WITH COMMON KEY
SP25
SP26
NEXT AUTHENTICATION REQUEST?
YES
NO
OBTAIN ELECTRONIC PRICED INFORMATION FROM SECURITY SERVER
SP27
STORE ELECTRONIC PRICED INFORMATION IN IC CARD
SP28
SEND ELECTRONIC PRICED INFORMATION TO BROWSER
SP29
END
SP30

FIG. 14


START
SP41
OBTAIN COMMON-KEY CORRESPONDING TO USER ID
SP42
SEND AUTHENTICATION REQUEST TO ENCRYPTION MODULE
SP43
RECEIVE RESULT OF AUTHENTICATION
SP44
SP45
HAS IC CARD BEEN AUTHENTICATED?
NO
YES
OBTAIN PRIVATE KEY FROM USER CERTIFICATE DATA BASE
SP46
DECRYPT ELECTRONIC PRICED INFORMATION
SP47
SEND IC-CARD WRITING REQUEST
SP48
SEND ELECTRONIC PRICED INFORMATION
SP49
END
SP50